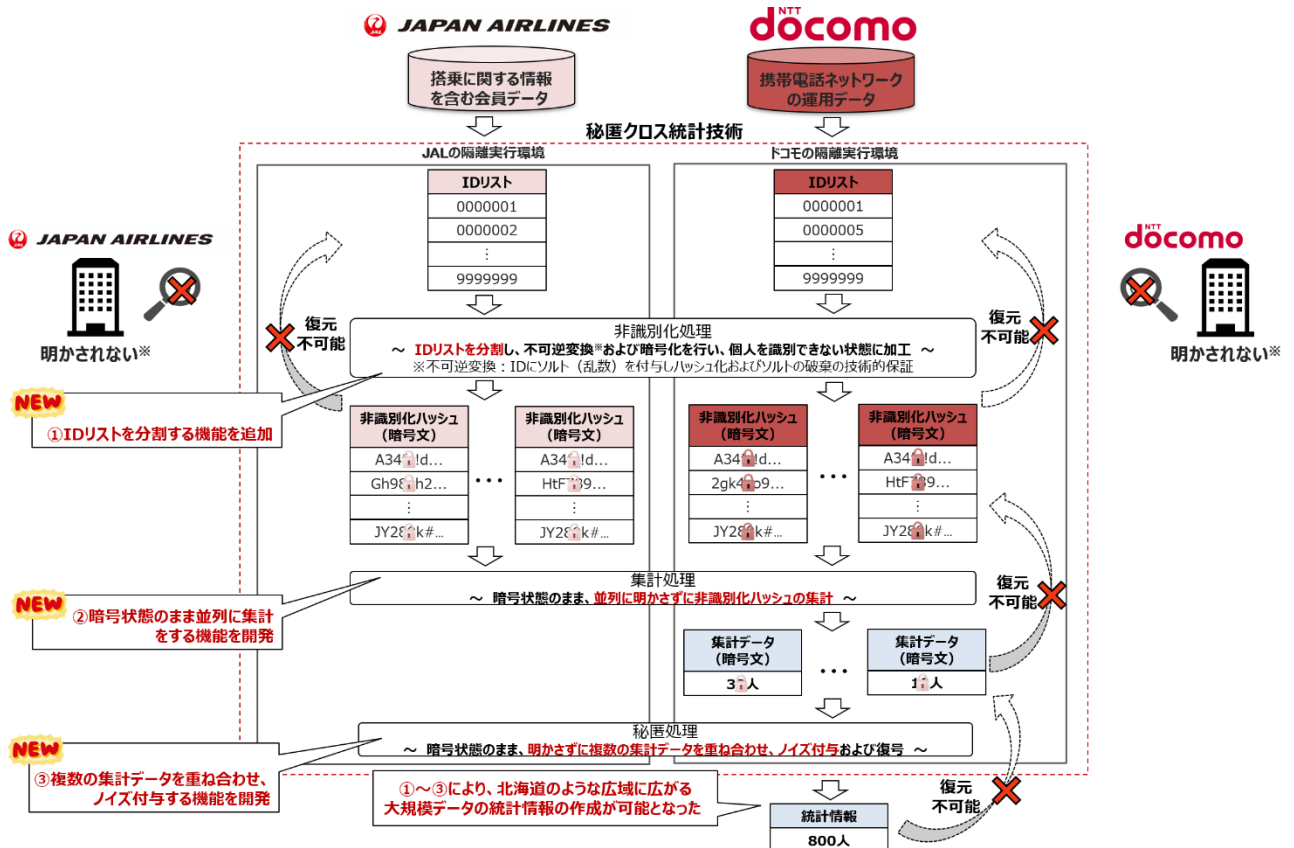


## 秘匿クロス統計技術とその進化

秘匿クロス統計技術は、相互にデータを明かさない状態で安全な統計情報を作成することを可能にする、NTT グループが推進する次世代 ICT 基盤構想「IOWN<sup>®</sup>」の構成技術です。本実証実験では、本技術を用いて、JAL、ドコモが、各社が保有する同じ形式の ID リストを、それぞれの安全な処理環境（隔離実行環境）で非識別化処理（不可逆変換および暗号化）を行い、個人を識別できない状態に加工した上で、暗号状態のまま集計処理と秘匿処理を実施します。

本実証実験では、広域を対象とした人口統計情報を作成するために、ドコモは上記処理方法などを用いることで安全性を維持した上で大規模な入力データに対しても有用性を低下させずに高速に集計する機能を実現しました。この機能は、入力データを分割および非識別化処理した上で、暗号状態で複数の入力データを集計処理し、暗号状態のまま処理結果を重ね合わせて、一つの集計結果を作成するというものです。これにより、集計処理を並列して実行することが可能となり、処理性能向上を実現しました。また、複数の入力データに対しても、一回の秘匿処理で安全性を保証することができ、有用性の低下を防ぐことができるようになりました。この機能により、北海道のような広域に広がる大規模データに対しても本技術の適用が可能となり、今回の実証実験を実施することができるようになりました。



※明かされないとは、一連の処理を人の目に触れることなく機械が行うことを技術的に保証することを指す

人口統計情報は、集団の人数のみを表す統計情報であり、作成される統計情報以外の情報は JAL、JAL カード、HAC、ドコモのいずれも確認することはできません。

本技術の安全性は、日本電信電話株式会社の研究成果である高速・安全なデータ結合処理技術<sup>※6</sup>に加えて、ドコモが保有する差分プライバシー<sup>※7</sup>に基づくプライバシー保護技術を併用することで実現しています。

本技術は、「モバイル空間統計」のガイドラインに準拠しており、非識別化処理、集計処理、秘匿処理を通じて統計情報を作成します。また、モバイル空間統計ガイドラインの中でご案内している「運用データ利用停止手続き」を行っているお客さまのデータは、本実証実験において利用しません。

※6 データを暗号化したまま処理できる暗号方式（準同型暗号）を応用し、複数の主体がおのおの持つデータを互いに明かさずに、データ結合処理と統計情報の作成を行う技術です。

※7 特定の背景知識や攻撃能力を持つ攻撃者に対しても安全性を保證できることを目的として作成されたプライバシー保護の強度を定量的に測る指標です。なお、米国国勢調査においても、「差分プライバシー」を用いた保護手法が採用されています。

\*「IOWN」は、日本電信電話株式会社の商標または登録商標です。